Information Security Management Office
Truman Building, Suite 280

FrontLine

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION SYSTEMS

Summer 2002

INSIDE

Hacking humans instead of computers

You take your job seriously. You certainly take your pay check seriously. You show up for work everyday. You have a professional attitude, you have a sense of propriety, you take the enterprises commitment to customer service seriously. You know your own job pretty well, you even know quite a bit about the tasks of those who surround you in your group.

Late one afternoon, you get a phone call or an e-mail. Someone whose name you recognize or think you should recognize wants something from you immediately.

The information the person wants so much could seem sensitive or it could seem harmless. Maybe it's your password or someone else's, maybe it's an unlisted phone line, maybe it's an important date, maybe it's the version number for the network operating system, maybe it's a physical access code, maybe it's the dial-in information for a conference call.

Maybe there is an urgency in the voice at the other end or some evocative exclamation points in the e-mail message. Maybe the person at the other end appeals to your desire to help someone out of a jam.

Maybe the inquirer has caught you just as you were leaving to go pick up your kid and you do not have time to think through why you shouldn't just blurt out the information they have requested.

Maybe the caller is not desperate; maybe the caller is intimidating. Maybe you are new on the job, or your position is shaky, or you are just one of those people whose self-confidence wavers when confronted with such hostility.

Maybe it's not late in the day, maybe it's right after lunch instead and all the blood has gone into digesting a burger and french fries. Maybe you are a little sleepy and a little distracted.

Whatever the reason, whatever the circumstances, you give up the information. Maybe you feel the person's pain, maybe you fear the person's clout, maybe you just can't be bothered, maybe you just didn't think it through. But after you hang up the phone, or hit the send button, you get that awful feeling. "Oh, no. I don't feel good about this." Tell someone immediately. It is quite possible you have been the victim of a "social engineering" attack. If you are wrong, everyone in the know will respect you for your forthrightness and your sense of responsibility. If you are right, you could be a hero. Because the intelligence that hackers gain from such attacks often leads to big losses and lots of woes for the companies or government agencies targeted.

Social engineering (i.e. lying, misrepresenting facts, impersonating authorized personnel or third-party personnel, conning, etc.) to get the intelligence needed to launch a cyber attack or commit some cyber fraud is as old as hacking itself. No technology can prevent against it. Firewalls, encryption, intrusion detection are all helpless against it. Only you stand between the hacker and the information they are looking for in a social engineering attack.

Social engineering attacks are not just aimed at individual users. They are often aimed at whole groups of users. For example, in the early 1990s, all the subscribers to a New York internet service provider received the following e-mail message: "It has been brought to my attention that your

account has been 'hacked' by an outside source. The charges added were significant, which is how the error was caught. Please temporarily change your password to 'DPH7' so that we can judge the severity of the intrusion. I will notify you when the problem has been taken care of. Thank you for your help in this matter." It was signed, "System Administrator."

Of course, the originator of the e-mail blast was not the system administrator, but a clever hacker who had conceived of a psychologically disarming social engineering scheme to have his victims change their passwords, instead of trying to guess it or using social engineering to elicit it from them (which might have proved more difficult).

Social engineering techniques have also been incorporated into virus and worm attacks in the last few years. Remember the "I LOVE YOU" worm? It arrives in your e-mail inbox, seemingly sent by someone whose e-mail address you recognized, with a subject head "I love you" that most people would find either endearing enough or puzzling enough to lead them to open the attached file and thus infect their computers and become unknowing accomplices in the spreading of the contagion.

Recognize the tell-tale signs

Here are some of the tell-tale signs that should alert you to the possibility of a social engineering attempt.

❒ Reluctance to provide contact information: If you say, "Can I have a number to call you back?" You might well hear a click. They'll just try the next stooge. Or maybe they'll say, "I'm on a cell phone, my battery's dying. I'll call you back in an hour after you gather this information for me." Or they'll say, "I'm on an 800 number, but it only works inside the state and I'm outside of it."

❒ Rushing: Is the person on the other end of the line really in a rush? They might say, "Hey, somebody's waiting for this!" Are they pushing you too hard? Are they screaming at you? That should give you pause to ponder.

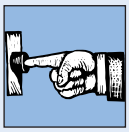
❒ Name-dropping: Remember, a social engineer might have a copy of your organization's internal phone list or even your annual report at his fingertips. And they might not use something as obvious as the name of a senior manager; instead they might use the spouse's name.

❒ Intimidation: Is the caller bullying you? Has your job been threatened? They might say, "I've been transferred four times, let me have your name, if you don't help me..."

❒ Small mistakes: Listen for misspellings, misnomers, odd questions and other blunders. For example, a hacker called a financial institution and said, "Hi, I'm your fraud representative from the Florida office. Your password's been in use for six weeks and..." But the company's systems happened to change passwords every 30 days.

❒ Requesting forbidden information: If someone says they need your password, they're lying. Don't give it to them. There are also other kinds of information that are so sensitive that you should know not to give them over to anybody you don't know—for example, your strategic plan, your earnings information prior to announcement, your new products information prior to release, etc. You should ask your organization's information security professionals for some guidelines in regard to proprietary information.

How to Combat Social Engineering



Here are some useful tips on how to foil the designs of social engineers.

❒ Verify the identity of callers. If you can't immediately identify them, insist on calling them back. If it's really an important call from an important person, they too will be concerned about the security of your organization and respect your precautions.

❒ Don't give out information about other employees–for example, names, staff positions, locations or telephone numbers–particularly if they are information systems personnel (MIS director, network administrator, PC support technician) or administrative personnel (financial officers, purchasing agents or payroll clerks). Instead, take a message and route it to the appropriate person.

❒ Don't discuss computers, software or communications equipment with those identifying themselves as vendor support for hardware or software, or as representatives of survey companies, personnel agencies or other outside services unless you know them or can verify both their identities and their need to know.

❒ If you do deduce that the caller is a hacker, consider leading the intruder into a trap or providing them with misinformation. Befriend them, let them hear you 'smiling' back at them, act as if you believe their story, promise to provide them with the information they seek, and tell them to hold on or call back.

❒ If you feel you've thwarted an attempt at social engineering, report the incident to your manager or to security personnel immediately.

❒ If you feel you've been tricked (even in the past), don't bury your head in the sand and hope that the problem just goes away. Report the incident immediately. Don't wait to see if anything bad happens. The information that has been purloined from a conversation with you may not be used right away or even in the manner that seems most apparent to you.

❒ Be sure to learn your organization's information security policies for users. Ask your manager or information systems personnel for a copy.

❒ Familiarize yourself with hacker social engineering tactics. Then when you get a call from way out in left field, ask yourself how the caller's identity, the story you've been presented and the request being made match what you know about any of these tactics.

❒ Care, but be aware. Don't let yourself be manipulated. When someone calls asking for help in some way that is unusual, put them on hold. Take a moment or two to think about what you're going to do.

❒ Be sure to ask your organization's information security staff for further guidance if you get suspicious.

Voice-Mail Security

Voice mail security checklist

Two days before Hewlett-Packard shareholders voted on the company's purchase of Compaq Computer, HP Chief Executive Carly Fiorina left an urgent voice mail for another top executive, telling him that they might have to "do something extraordinary" to persuade two investors to support the hotly contested deal.

In the message to Chief Financial Officer Bob Wayman, Fiorina said HP's chief vote collector was worried about the way two large investors, Deutsche Bank and Northern Trust, were planning to vote their shares. "We may have to do something extraordinary for those two to bring 'em over the line here," she says.

The voice mail reveals some of the intense last-minute lobbying by Fiorina and other executives before the March shareholder vote, which was so close that both sides are awaiting an official independent tally.

What the company did in the final days and even hours before the polls closed is at the center of a lawsuit filed by dissident shareholder and board member Walter Hewlett, who led efforts by the Hewlett and Packard families to defeat the $19 billion deal.

Wayman confirmed that the message, which was left anonymously on a *San Jose Mercury News* reporter's voice mail, was authentic.

In contrast to the dangers of Trojan horses, viruses, Web site hacks and other cyber attacks, your organization's voice mail system may seem like the least of your concerns—but it is indeed an area of vulnerability often exploited by hackers and industrial spies.

Here are some tips to keep in mind.

❒ When you first receive voice mail privileges, you should change your password immediately. And, just as with your e-mail account and network access, you should take care to create a password that will be difficult for a hacker, a corporate spy or a malcontented co-worker to guess. Come up with a password that is easy for you to remember, but difficult for someone else to guess. Use a clever mix of letters and numbers.

❒ Change your password frequently. Remember, your voice mail account is on the frontline of information systems security—no matter how strong your password is, you should still change it regularly.

❒ Don't share your password with anyone.

❒ Record a personalized greeting in your own voice.

❒ Delete messages after you've listened to them. Otherwise, you're simply leaving more information around for an intruder to listen to.

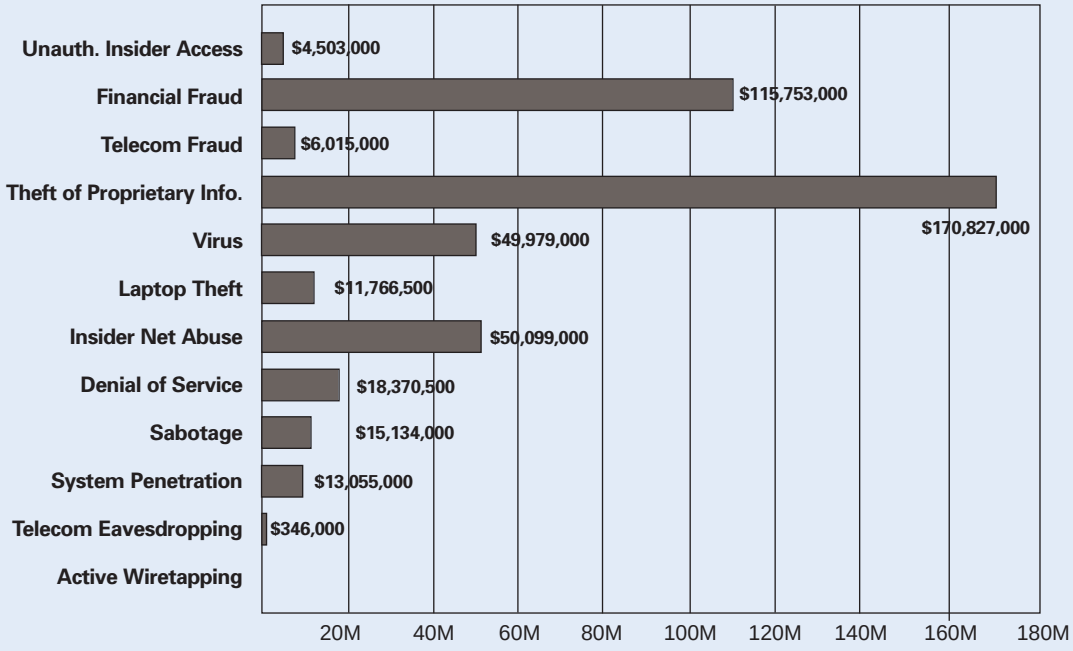
❒ Don't leave messages that contain sensitive, confidential or personal information in a voice mail box. And when someone else does so in your voice mail box, take the opportunity to educate them about the grim realities of telecommunications security.

❒ If you know of a still-active voice mail box for an employee that has been terminated or transferred, notify your information security personnel or other appropriate authority immediately.

❒ Report strange or suspicious voice mail messages to your supervisor or other appropriate authority immediately. Don't delete such messages—they may yield vital evidence.

❒ Take the time to study the voice mail system instructions. Learn the ins and outs of your voice mail systems. This knowledge will help you detect breaches in telecommunications security.

Proof-Positive
Dollar Amount of Losses by Type



CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

2002: 223 respondents/44%

Horror Stories

Headlines throughout the world abound with tales of cyberspace crimes, misdemeanors, blunders, lapses and snafus. These real-world horror stories make the diverse threats to your organization tangible and poignantly clear.

Melissa creator gets 20 months

The creator of the "Melissa" virus was sentenced Wednesday to 20 months in federal prison for causing millions of dollars of damage by disrupting e-mail systems worldwide in 1999. DAVID L. SMITH, 33, pleaded guilty in December 1999 to a state charge of computer theft and to a federal charge of sending a damaging computer program. In the federal plea, both sides agreed the damage was greater than $80 million.

FAA confirms hack attack

Hackers were able to penetrate a Federal Aviation Administration system earlier this week and download unpublished information on airport passenger screening activities, federal officials confirmed.

Styling themselves "The Deceptive Duo," the hackers publicly defaced an FAA server used by what was the administration's Civil Aviation Security organization, which until recently was responsible for supervising passenger screening at U.S. airports. There, the intruders posted a mission statement vowing to expose America's poor state of cyber security for the good of the nation.

"Tighten the security before a foreign attack forces you to," the Duo extolled. "At a time like this, we cannot risk the possibility of compromise by a foreign enemy."

At the bottom of the page, the defacers included a screen-shot showing a portion of a Microsoft Access database, with each row displaying the three-letter code for a different U.S. airport, the name of an FAA inspector, a screener I.D. number, the number of passengers the screener handled, and the number of guns, explosives or chemicals he or she intercepted.

Turkish religious affairs site hacked by 'Satanists'

The official Internet site of the Religious Affairs Directorate has been hacked by satanists.

According to Hakan Topuzoglu, a founder of the Turkish Internet Union, those who tried to access the site of the Religious Affairs Directorate at diyanet.gov.tr, encountered the character of "Gambit" from the famous cartoon X-Man who holds playing cards and who defeats his enemies by hurling these cards at them.

The hacked site also carries an English-language text, noting that this is a very ugly site and those who wish to express negative views about it should e-mail their messages to satanics.souls@yahoo.com.br.

Europe bans spam

The European Parliament has voted to ban the sending of unsolicited commercial email. The new European directive should be in place some time next year and would mean that people will have to "opt in" or ask to receive commercial email.

Frontline 8/02

For the fourteenth consecutive year, the National Association of Chief Information Officers, NASCIO, will honor outstanding achievements in the field of information technology through its Recognition Awards Program. Missouri's State Security Committee (SSC) has been nominated for an award in the Security and Business Continuity category. Missouri's Information Technology Advisory Board (ITAB) formed the SSC in February, 2000, to provide guidance on the confidentiality, integrity, availability and authenticity of Missouri state government information and dependent resources.

The SSC provides the state and its citizens intrinsic benefits through continued and improved information security, confidence and trust, but primarily serves to advise ITAB and state entities on issues applicable to information security in the following ways:

- Acts as an authoritative source for opinions, practices and principles for information owners, custodians, users, security practitioners, technology products and systems.
- Defines, establishes and maintains coordination with other information security practitioners; i.e., ISSA, ISC2, NIST, CERT, NPIC, InfraGard, etc. and security stakeholders.
- Promotes information security and awareness.
- Provides a network to improve intra-governmental information security in the State of Missouri.
- Proposed, lobbied for and secured passage of legislation to clarify the exemption of computer security related information from disclosure under Missouri's Sunshine Law.
- Championed a Computer Incident Reporting Policy and Procedures that all executive branch agencies have agreed to follow.
- Drafted information security principles to guide agencies when developing policies and standards.
- Working with ITAB's Statewide Information Architecture Committee to establish guidelines and standards within a security domain.
- Created INFOCON (INFormation Operations CONdition) for Missouri state entities, a plan that quantifies cyberthreats to the critical information infrasturucture and recommends actions to uniformly heighten or reduce network defensive posture, to defend against computer network attacks and to mitigate sustained damage to the State's information infrastructure. The INFOCON system will support all personnel who use State of Missouri information systems, coordinating the overall defensive effort through adherence to a set of security guidelines.

The IT Directors from the various state agencies, commissions, offices, colleges and universities comprise the ITAB membership. Each ITAB member is allowed to nominate a primary and alternate voting member to the SSC.

